

# SIP-0012: Provide treasury funds to FastBTC

## Background:

We recently reactivated an improved version of FastBTC to allow for quick and simple user onboarding. At this point, FastBTC is limited to 0.01 BTC per transaction, because of missing liquidity. It is proposed to transfer 100 BTC from the Origin BTC Multisig Wallet through the RSK 2-way-peg onto the RSK chain. The funds are to be held by the Exchequer Multisig Wallet and supplied to the FastBTC contract in batches as liquidity requirements rise.

The FastBTC contract is a very simplistic, non-upgradable contract. It just knows 2 roles: owner and admin. Both can withdraw funds from the contract. The owner can additionally replace the admin. The Bitocracy is acting as the owner and a 3 out of 5 multisig is set as admin (0x0f279e810b95e0d425622b9b40d7bcd0b5c4b19d). The key holders are active team members (whose tokens could be slashed by the Exchequer multisig in case of misbehaviour) and early funders. 4 of the addresses have been set already and a 5th address is going to be added within the next week:

- 0x986C65fc1783a445CecCadE74234dC8627d429d8
- 0x0b3be9435610aac0e1c6f7a26c77e2213738cb48
- 0xb66fb8937aecdb12210b384120e2b4ba506b3140
- 0xc39ef4a81c57d5866924e6cc6c260c617ef7287d

Incoming BTC are being held by a multisig with following keyholders:

- xpub6BfKEBjxckgv5wSMRfo1Xs4GQPrPnmpBCMr5Ks4sodwyFHHv46YuUTLXkTxjvY17m1yicc7P9GuRvxTL3g9QyLVvGN6LoyewBXVmeBjKpnV
- xpub661MyMwAQrbcGzaYcTzVwawoUX1ha8k81vbhN7RQuaL3qb4jrowz6ytfEmXvb g3sFZVKyMLp7MW8KCXY36yzJgsx7QT6mxHaRNYScQLvKKs
- xpub6DXfjxAVvM3Bhc3SMjtFxTgXrTm6KvMX4v5LcjAhzULVCeazmr3Az6iwpJ3upwT1dTRDjKs4X7GsWyFzryUa8pMQxVyHGSBoehxEPW5oyZ5
- xpub6D7UgjtGH1Jz5DiiWYUWmojWGnaR5dYfDNzmwGxmtKxs9815n5bnsgodr6g6JyX7H2Q4CHRC8YHjC445s1VoAT1CUF8MawR3jQX67JRDxa
- xpub661MyMwAQrbcFLXXK8g24KqYv5TdGK9wd6wPmCJkkidFwmuKpEH41XVxV6CJTL4cmcMiDnNNF1dtWQBkQ7k9U6yuFULibdqriF8CHJfCH
- xpub6BgUF1rCKuijQqc8gUUSsS3pCCfeyqA8VfJvBcfXxLjMFHycooFHWeay95g33NcMV3vg6q2jKw3PLmKBeJSfBAiikYjJGjAgCZt5i41PD2H
- xpub6C2rAfZ1QCurnA5pGvb1ra6mzceakedwMZ4s9STy178HPUGDQj7ajxqsSMhM4hxnGWbhccdf3HZVnnWhXhHCEguef16RdWYGDnqzMiJgA3

For each user a unique deposit address is derived from this multisig. If liquidity on RSK is running low, the funds need to be transferred via the RSK 2-way-peg in order to refill the contract.

Because of the way the RSK 2-way-peg is designed, the multisig cannot send the funds over the peg directly, but we need to use a single private key. This means that for a time period of 24h the assets to be transferred are being controlled by a single person. This is why the amount is to be transferred in batches and the person(s) in charge should be slashable by governance in case of misbehaviour (and therefore have enough at stake).

Providing liquidity for FastBTC is not just substantially improving the user onboarding process, but also a lucrative business for the protocol, because fees are generated on each transfer.

## Resolved:

1. Transfer 100 BTC from the Origin BTC Multisig Wallet through the RSK 2-way-peg onto the RSK chain. The transfer is to happen in batches and executed by slashable SOV holders.
2. The funds are to be held by the Exchequer multisig (0x924f5ad34698fd20c90fe5d5a8a0abd3b42dc711) until they are provided to the FastBTC contract (0xca1c5b1bc55755c5e3b6ed1afe88abd7b26f147f).
3. 10 RBTC are to be provided to the FastBTC contract immediately and the transfer limit is to be increased to 0.1 BTC.
4. Funds are to be moved from the BTC multisig in charge of receiving the user deposits whenever liquidity on the FastBTC contract is beginning to run low.
5. After 4 weeks of operation and a completed audit report of the FastBTC backend, the limits are to be lifted completely and the remaining 90 RBTC are to be transferred.